



UNITED STATES PATENT AND TRADEMARK OFFICE

MN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/710,327	07/01/2004	David S. Bonalle	70655.2500	4326
66170	7590	05/25/2007	EXAMINER	
AMERICAN EXPRESS TRAVEL RELATED SERVICES CO., INC. c/o SNELL & WILMER, L.L.P. ONE ARIZONA CENTER 400 E. VAN BUREN STREET PHOENIX, AZ 85004-2202			CHAI, LONGBIT	
		ART UNIT	PAPER NUMBER	
		2131		
		MAIL DATE	DELIVERY MODE	
		05/25/2007	PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/710,327	BONALLE ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 22 March 2007.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-46 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-46 is/are rejected.
- 7) Claim(s) 2 and 19 is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 01 July 2004 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 3/22/2007.
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) Notice of Informal Patent Application
- 6) Other: _____

DETAILED ACTION

Priority

1. No claim for priority has been made in this application.

The effective filing date for the subject matter defined in the pending claims in this application is 7/1/2004.

Claim Objection

2. Claims 2 and 19 are objected because the claim language "said sensor" should be replaced with "said keystroke scan sensor" to be consistent with other claims (e.g., claim 3 and 4) that also use "said keystroke scan sensor" instead of "said sensor". Appropriate corrections are required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 6 recites the limitation "said database". There is insufficient antecedent basis for this limitation in the claim. Examiner notes It is suggested to replace claim 6 dependency on claim 4 with claim 5 (i.e. replace "The smartcard transaction system of claim 4" with "The smartcard transaction system of claim 5") that can provide proper / better antecedent basis for claim 6.

Double Patenting

The nonstatutory provisional double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4. Claim 1 – 8, 11 – 42 and 44 – 46 are rejected under the judicially created doctrine of obviousness-type provisional double patenting as being unpatentable over claim 1 – 8, 11 – 42 and 44 – 46 of U.S. Patent Copending Application No 10/708,831. Although the conflicting claims are not identical, they are not patentably distinct from each other because (a) the instant application is directed toward a smart card and the copending application is directed toward a transponder; however, both types of media

are considered and recognized as obvious and conventional types of media for communicating and (b) the instant application is directed toward a keystroke scan sample and the copending application is directed toward a hand geometry sample; however, both types of biometric identification method are considered and recognized as obvious and alternative types of authenticating for an individual. Therefore, such differences would have been well known within the skill in the art at the time of invention, especially as prior art discloses smart cards, transponders, and different biometric identifications being interchangeable, for design choice, system constraints, cost, convenience, and etc. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Furthermore, for the similar reasons, Examiner notes claims 1 – 8, 11 – 42 and 44 – 46 of the instant application are also provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 – 8, 11 – 41, 43 and 45 – 47 of copending Application No. 10/710,329 and 10/710,328, 10/710,311 and unpatentable over claims 1 – 8, 11 – 42 and 44 – 46 of copending Application No. 10/710,325, 10/710,324 and 10/708,832 and claims 1 – 35 of copending Application No. 10/708,837.

Additionally, for the similar reasons, Examiner notes claims 1 – 8, 11 – 42 and 44 – 46 are also rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 – 8, 11 – 41, 43 and 45 – 47 of U.S. Patent No 7,059,531 and unpatentable over claims 1 – 8, 11 – 42 and 44 – 46 of U.S. Patent No 7,121,471.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1 – 2, 4 – 6, 8, 9 11 – 15 and 19, 20, 22, 24 – 32 and 34 – 37, 39 – 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nambiar et al. (U.S. Patent 2002/0128977), in view of Ito et al. (U.S. Patent 6,657,614).

As per claim 1, 22 and 34, Nambiar teaches a smartcard transaction system configured with a biometric security system (Nambiar: Figure 1 / Element 14 & 100), said system comprising:

a smartcard configured to communicate with a reader (Nambiar: Para [0007]);
and

a reader configured to communicate with said system (Nambiar: Para [0020] Line 6 – 10: a smart card reader is used to access the security data stored at the smart card and the security data is further used by the system for authentication purpose).

However, Nambiar does not disclose expressly a keystroke scan sensor configured to detect a proffered keystroke scan sample, said keystroke scan sensor configured to communicate with said system.

Ito teaches a keystroke scan sensor (Ito: Figure 2 & 7, Figure 1 / Element 10, Column 8 Line 55 – 56: a biometric keystroke scan sensor to catch different key stroke behaviors and timing information from different individuals) configured to detect a proffered keystroke scan sample, said keystroke scan sensor configured to communicate with said system (Ito: Column 6 Line 27 – 35, Column 8 Line 1 – 5 / Line 11 – 14 and Column 12 Line 47 – 55); and,

a device (Ito: Figure 1 / Element 70: judging result signal processing unit) configured to verify said proffered keystroke scan sample to facilitate a transaction (Ito: Column 4 Line 30 – 35 / Line 36 – 43, Column 6 Line 36 – 50 and Column 13 Line 51 – 54 / Line 55 – 61: a transaction is authorized after the verifications of biometric keystroke scan samples – e.g., the finger timing movements and pressing forces of the individuals).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ito within the system of Nambiar because (a) Nambiar teaches the smart card transaction system that can use all different options of user identifications such as cryptographic digital signatures, and biometric signatures to authorize a online transaction (Nambiar: Para [0020]), and (b) Ito teaches providing alternative type of biometric personal identification that can offer much greater accuracy for individual by using biometric keystroke scan samples – e.g., the finger timing movements and pressing forces of the individuals for authentication purpose (Ito: Column 8 Line 10 – 13 and Column 6 Line 34 – 35).

As per claim 2 and 35, Nambiar as modified teaches said sensor is configured to communicate with said system via at least one of a smartcard, a reader, and a network (Nambiar: Para [0026] Line 12 – 17 and Para [0025]: The smart card reader authentication system can include a biometric device for authenticating the user via a network for client transaction verifications).

As per claim 4, Nambiar as modified teaches said keystroke scan sensor is configured to log at least one of a detected keystroke scan sample, processed keystroke scan sample and stored keystroke scan sample (Ito: Figure 26 / Element 312 and Column 16 Line 6 – 10).

As per claim 5, Nambiar as modified teaches including a database configured to store at least one data packet, wherein said data packet includes at least one of proffered and registered keystroke scan samples, proffered and registered user information, terrorist information, and criminal information (Nambiar: Para [0025] Line 5 – 15 & Figure 1: The smart card authentication system can operate via a network for a online transaction process).

As per claim 6 and 27, Nambiar as modified teaches said database is contained in at least one of the smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system (Nambiar: Para [0020]: at least, the PIN and biometric signatures can be stored in a smart card).

As per claim 8, 25 and 36, Nambiar as modified teaches said keystroke scan sensor device is configured with at least one of an electronic sensor, an optical sensor and a keyboard (Ito: Column 10 Line 29 – 35).

As per claim 9, 30 and 43, Nambiar as modified teaches said keystroke scan sensor is configured to detect and verify keystroke scan characteristics including at least one of behavioral, temporal and physical characteristics (Ito: Column 4 Line 30 – 35 / Line 36 – 43).

As per claim 11, 28 and 42, Nambiar as modified teaches including a device configured to compare a proffered keystroke scan sample with a stored keystroke scan sample (Ito: Figure 25 / Element 414 and Column 15 Line 8 – 14).

As per claim 12, 29 and 46, Nambiar as modified teaches said device configured to compare a keystroke scan sample is at least one of a third-party security vendor device and local CPU (Ito: Figure 215 / Element 100 & 70: local CPU).

As per claim 13, Nambiar as modified teaches a stored keystroke scan sample comprises a registered keystroke scan sample (Ito: Column 14 Line 16 – 22 and Column 13 Line 32 – 35).

As per claim 14, Nambiar as modified teaches said registered keystroke scan sample is associated with at least one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal

account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information (Ito: Column 13 Line 32 – 35 / Line 43 – 50).

As per claim 15, Nambiar as modified teaches different registered keystroke scan samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information (Ito: Column 13 Line 32 – 61: different registered keystroke scan samples are stored by numerous individuals, who inherently have different personal information).

As per claim 19, Nambiar as modified teaches said sensor is configured to provide a notification upon detection of a sample (Ito: Column 14 Line 40 – 45: outputting a signal to the display screen).

As per claim 20, Nambiar as modified teaches said device configured to verify is configured to facilitate at least one of access, activation of a device, a financial transaction, and a non-financial transaction (Nambiar: Para [0007]: a transaction).

As per claim 24, Nambiar as modified teaches said step of registering further includes at least one of: contacting said authorized sample receiver, proffering a

Art Unit: 2131

keystroke scan to said authorized sample receiver, processing said keystroke scan to obtain a keystroke scan sample, associating said keystroke scan sample with user information, verifying said keystroke scan sample, and storing said keystroke scan sample upon verification (Ito: Column 13 Line 45 – 55: keystroke scan sample with user information).

As per claim 26 and 37, Nambiar as modified teaches said step of proffering further includes proffering a keystroke scan to a keystroke scan sensor communicating with said system to initiate at least one of: storing, comparing, and verifying said keystroke scan sample (Ito: Column 13 Line 45 – 55).

As per claim 31 and 41, Nambiar as modified teaches said keystroke scan sensor device is configured to detect at least one of false keystrokes and body heat (Ito: Figure 25 / Element 414 and Column 15 Line 8 – 14: detect false keystrokes).

As per claim 32 Nambiar as modified teaches said step of proffering a keystroke scan to a keystroke scan sensor communicating with said system to initiate verification further includes at least one of detecting, processing and storing at least one second proffered keystroke scan sample (Ito: Column 14 Line 24 – 34 and Column 4 Line 30 – 35 / Line 36 – 43: a second proffered keystroke scan sample is considered as either single click / double click or timing / pressing force measurement).

As per claim 39, Nambiar as modified teaches said step of detecting further includes logging each proffered keystroke scan sample (Ito: Figure 26 / Element 312 and Column 16 Line 6 – 10).

As per claim 40 Nambiar as modified teaches said step of detecting further includes at least one of detecting, processing and storing at least one second proffered keystroke scan sample (Ito: Column 14 Line 24 – 34 and Column 4 Line 30 – 35 / Line 36 – 43: a second proffered keystroke scan sample is considered as either single click / double click or timing / pressing force measurement).

As per claim 44 Nambiar as modified teaches comparing a proffered keystroke scan sample with a stored keystroke scan sample includes comparing a proffered keystroke scan sample with a biometric sample of at least one of a criminal, a terrorist, and a cardmember (Nambiar: Para [0005] Line 6 – 8: a cardholder).

As per claim 45 Nambiar as modified teaches said step of verifying includes verifying a proffered keystroke scan sample using information contained on at least one of a local database, a remote database, and a third-party controlled database (Ito: Column 15 Line 17 – 19 and Column 13 Line 55 – 56: personal data (the vector and matrix – i.e. keystroke scan samples) stored in RAM is considered as a local database).

6. Claims 3, 18 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nambiar et al. (U.S. Patent 2002/0128977), in view of Ito et al. (U.S. Patent 6,657,614), and in view of Goodman et al. (U.S. Patent 2002/0043566).

As per claim 3 and 38, Nambiar as modified does not disclose expressly said keystroke scan sensor is configured to facilitate a finite number of scans.

Nambiar / Ito in view of Goodman teaches said keystroke scan sensor is configured to facilitate a finite number of scans (Goodman: Para [0029] Line 7 – 11: after a predetermined number of scan, the transaction card is deactivated & Ito: Figure 2).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Goodman within the system of Nambiar as modified because (a) Nambiar teaches the smart card transaction system that can use all different options of user identifications such as cryptographic digital signatures, and biometric signatures to authorize a online transaction (Nambiar: Para [0020]), and (b) Goodman teaches providing a flexible and reliable protection mechanism by deactivating the transaction card if needed while allowing signature captures to be re-taken after a certain number of error attempts (Goodman: Para [0029] Line 7 – 11).

As per claim 18, Nambiar as modified does not disclose expressly said smartcard is configured to deactivate upon rejection of said proffered keystroke scan sample.

Nambiar / Ito in view of Goodman teaches said smartcard is configured to deactivate upon rejection of said proffered keystroke scan sample (Goodman: Para [0029] Line 7 – 11: after a predetermined number of scan, the transaction card is deactivated). See same rationale of combination applied herein as above in rejecting the claim 3.

7. Claims 7, 21, 23 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nambiar et al. (U.S. Patent 2002/0128977), in view of Ito et al. (U.S. Patent 6,657,614), and in view of Smithies et al. (U.S. Patent 6,091,835).

As per claim 7, Nambiar as modified does not disclose expressly said remote database is configured to be operated by an authorized sample receiver.

Nambiar / Ito in view of Smithies teaches said remote database is configured to be operated by an authorized sample receiver (Smithies: Column 30 Line 1 – 4, Column 15 Line 52 – 56, Column 41 Line 64 – Column 42 Line 7 and Column 32 Line 42 – 60: the APC (Authentication Policy Component) of a Transcript Generator Module that receives and stores signature captures is an authorized agent).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Smithies within the system of Nambiar as modified because (a) Nambiar teaches the smart card transaction system that can use all different options of user identifications such as cryptographic digital signatures, and biometric signatures to authorize a online transaction (Nambiar: Para [0020]), and

Art Unit: 2131

(b) Smithies teaches an enhanced security mechanism for a smart card transaction system by adding more than one different options of the signatures into the authentication template such as cryptographic digital signatures, digitized handwritten signatures and biometric signatures to authenticate a particular transaction (Smithies: Figure 4c, Column 31 Line 18 – 38 and Column 33 Line 10 – 14).

As per claim 21 and 33, Nambiar as modified does not disclose expressly said device configured to verify is configured to facilitate the use of at least one secondary security procedure.

Nambiar / Ito in view of Smithies teaches said device configured to verify is configured to facilitate the use of at least one secondary security procedure (Smithies: Figure 4c, Column 31 Line 18 – 38 and Column 33 Line 10 – 14: adding more than one different options of the signatures into the authentication template such as cryptographic digital signatures, digitized handwritten signatures and biometric signatures). See same rationale of combination applied herein as above in rejecting the claim 7.

As per claim 23, Nambiar as modified does not disclose expressly registering at least one keystroke scan sample with an authorized sample receiver.

Nambiar / Ito in view of Smithies teaches registering at least one keystroke scan sample with an authorized sample receiver (Smithies: Column 15 Line 52 – 56, Column 41 Line 64 – Column 42 Line 7 and Column 32 Line 42 – 60: the APC (Authentication Policy Component) of a Transcript Generator Module that receives and stores signature

captures is an authorized agent) & (Ito: Column 14 Line 16 – 22 and Column 13 Line 32 – 35). See same rationale of combination applied herein as above in rejecting the claim 7.

8. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nambiar et al. (U.S. Patent 2002/0128977), in view of Ito et al. (U.S. Patent 6,657,614), and in view of Black (U.S. Patent 6,307,956).

As per claim 10, Nambiar as modified teaches said keystroke scan sensor device is configured to detect false keystrokes (Ito: Figure 25 / Element 414 and Column 15 Line 8 – 14: detect false keystrokes). However, Nambiar as modified does not disclose expressly detecting body heat.

Black teaches detecting body heat (Black: Column 19 Line 58 – 63: detecting user's finger temperature is qualified as detecting part of a user's body heat).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Black within the system of Nambiar as modified because (a) Nambiar teaches the smart card transaction system that can use all different options of user identifications such as cryptographic digital signatures, and biometric signatures to authorize a online transaction (Nambiar: Para [0020]), and (b) Black teaches an enhanced security mechanism for validating biometric identifications by using additional sensors including measuring the user's finger temperature in order to access an account during a transaction (Black: Column 19 Line 58 – 63).

Art Unit: 2131

9. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nambiar et al. (U.S. Patent 2002/0128977), in view of Ito et al. (U.S. Patent 6,657,614), and in view of Moebs et al. (U.S. Patent 2005/0065872).

As per claim 16, Nambiar as modified does not expressly expressly a keystroke scan sample is primarily associated with first user information, wherein said first information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein a keystroke scan sample is secondarily associated with second user information, wherein said second information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein said second user information is different than said first user information.

Nambiar / Ito in view of Moebs teaches a keystroke scan sample is primarily associated with first user information, wherein said first information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, and wherein a keystroke scan sample is secondarily associated with second user information, wherein said second information

Art Unit: 2131

comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, and wherein said second user information is different than said first user information (Moebs: Para [0017] Line 1 – 4: the customer may avoid overdrafts also by pre-authorizing the financial institution to tie the customer's checking account to one or more of the customer's other accounts such as the customer's deposit saving accounts – i.e. Examiner notes two separate signature samples can be used for two separate account to avoid pre-authorizing the financial institution to tie a single signature sample to each account of a particular customer).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Goodman within the system of Nambiar as modified because (a) Nambiar teaches the smart card transaction system that can use two separate account number (i.e. a secondary transaction account number in addition to a primary account number) to limit exposure to online fraud (Nambiar: Para [0005] Line 10 – 17), and (b) Moebs teaches two separate authentication signature samples can be used for two separate account to avoid pre-authorizing the financial institution to tie a single authentication signature sample to each account of a particular customer (Moebs: Para [0017] Line 1 – 4: the customer may avoid overdrafts by pre-authorizing the financial institution to tie the customer's checking account to one or more of the customer's other accounts such as the customer's deposit saving accounts).

Art Unit: 2131

10. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 2002/0128977), in view of Ito et al. (U.S. Patent 6,657,614), and in view of Teicher et al. (U.S. Patent 6,257,486).

As per claim 17, Nambiar as modified does not disclose expressly said smartcard transaction system is configured to begin authentication upon verification of said proffered keystroke scan sample.

Nambiar / Ito in view of Teicher teaches said smartcard transaction system is configured to begin authentication upon verification of said proffered keystroke scan sample (Teicher: Column 7 Line 40 – 48: a mutual authentication is taken).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Teicher within the system of Nambiar as modified because (a) Nambiar teaches the smart card transaction system that can have two-factor authentication process – i.e. authenticate the smart card itself as well as validate the user identification information (Nambiar: Para [0008]), and (b) Teicher teaches providing an enhanced protection mechanism by employing mutual authentication techniques between the smart card and the smart card user (Teicher: Column 7 Line 40 – 48).

Art Unit: 2131

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788.

The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Longbit Chai, Ph.D.
Patent Examiner
Art Unit 2131
4/20/2007